In the Claims

1. (currently amended) A method for managing access to a network, comprising:

providing wireless communication in a network;

providing a plurality of distributed firewall ~~protection~~ units ~~between said network and a wireless access device~~ in the network, each firewall unit configured to provide wireless access to the network for a set of valid wireless access devices associated with the firewall unit;

~~submitting~~ receiving, at a particular one of the plurality of distributed firewall units, an identification code ~~to said network~~ transmitted wirelessly ~~from said~~ from a wireless access device, said identification code a media access control number ~~associated with and pertaining to said~~ of the wireless access device;

determining ~~the validity of~~ whether said identification code is valid for the particular firewall unit to grant network access to the wireless access device ;

granting ~~wireless~~ network access at the particular firewall unit to said wireless access device when said identification code is valid;

denying ~~wireless~~ network access at the particular firewall unit to said wireless access device when said identification code is not valid~~;~~

~~issuing an alert when said identification code is not valid~~.

2. (Original) The method described in Claim 1, wherein said providing said wireless communication is accomplished with an intelligent concentrator enabled for wireless communication.

3. (Original) The method described in Claim 2, wherein said providing said wireless communication is accomplished in circuitry resident in said intelligent concentrator.

4. (cancelled)

5. (currently amended) The method described in Claim 1, wherein said determining ~~said validity of~~ whether said identification code is valid is accomplished by reference to a list of valid identification codes associated with the particular firewall unit.

6. (currently amended) The method described in ~~Claim 2~~ claim 6, wherein said list of valid identification codes is resident in said ~~intelligent concentrator~~ firewall unit.

7. (Original) The method described in Claim 5, wherein said list of valid identification codes is resident in a server in said network.

8. (Original) The method described in Claim 1, wherein said denying said ~~wireless~~ access to said network at the particular firewall unit is accomplished simultaneously with granting access to ~~said~~ wireless accesses devices with valid identification codes.

9. (Original) The method described in Claim 1, wherein said network is a wireless personal area network.

10.-19. (cancelled)

20. (currently amended) An intelligent concentrator, comprising:

a housing configured to be mounted within a cavity in a wall, said housing including a first interface at an internal part of the wall and a second interface external to and substantially planar with en external part of the wall;

a cable connector coupled to said housing at the first interface and adapted to communicatively couple said intelligent concentrator to a network data cable;

electronic circuitry mounted in said housing enabled to wirelessly communicate with a wireless access device and a network; and

a distributed firewall resident in said electronic circuitry wherein said firewall is enabled to control the access to said network of said wireless access device only at the intelligent data concentrator by determining whether an~~, said control via a validated~~ identification code transmitted from said wireless access device is included in a set of valid identification codes identifying wireless access devices associated with the intelligent data concentrator, said identification code a media access control number associated with ~~and pertaining to~~ said wireless access device.

21. (Original) The intelligent concentrator described in Claim 20, wherein said intelligent concentrator is enabled as a hub of a personal area network.

22. (Original) The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to obtain a list of valid identification codes from a server in said network.

23. (cancelled).

24. (Original) The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to deny access to said wireless access device if said identification code is not valid.

25. (Original) The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to issue an alarm to a network manager is said identification code is not valid.